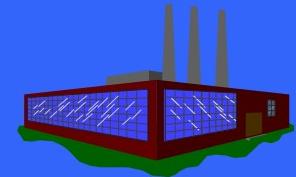


Defense Investigative Service



***A Briefing on the National Industrial Security Program
for Contracting Officers and Others
Supporting the Classified Procurement Process***

DIS & the Contracting Community



- *DIS provides security countermeasure expertise to industry on behalf of the U.S. military departments, Defense agencies, and non-DoD User Agencies*
- *DIS works in partnership with industry to establish and maintain security systems which provide protection to classified information*



Defense Investigative Service

1. Personnel Security Investigations Program

DIS Special Agents conduct the majority of personnel investigations

in the federal government serving both government and industry customers

Missions:



Defense Investigative Service

Two Principal Missions:

II. Industrial Security

Program

DIS has industrial security oversight and assistance responsibility for over 11,000 cleared facilities

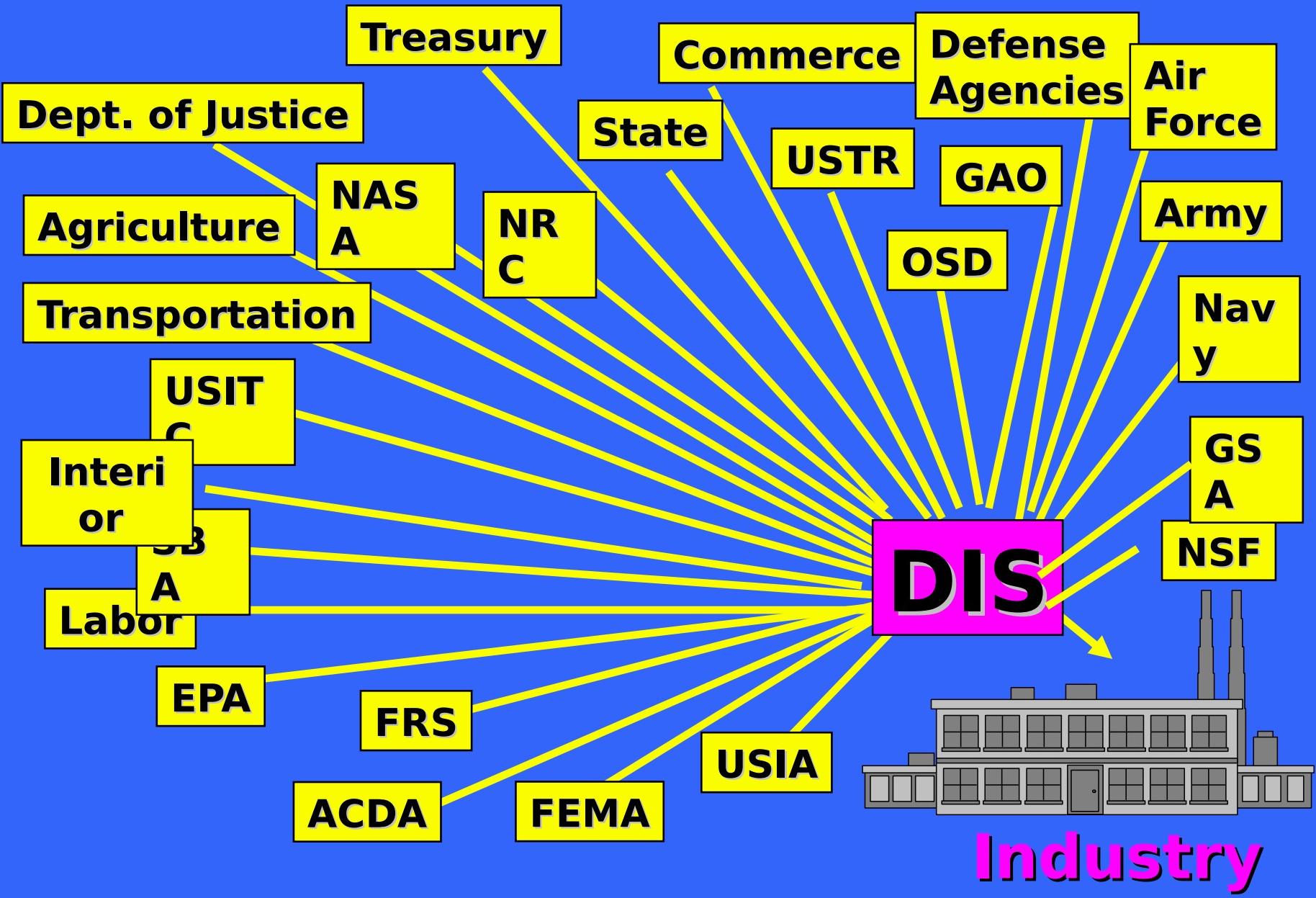
participating in the National Industrial Security Program (NISP)



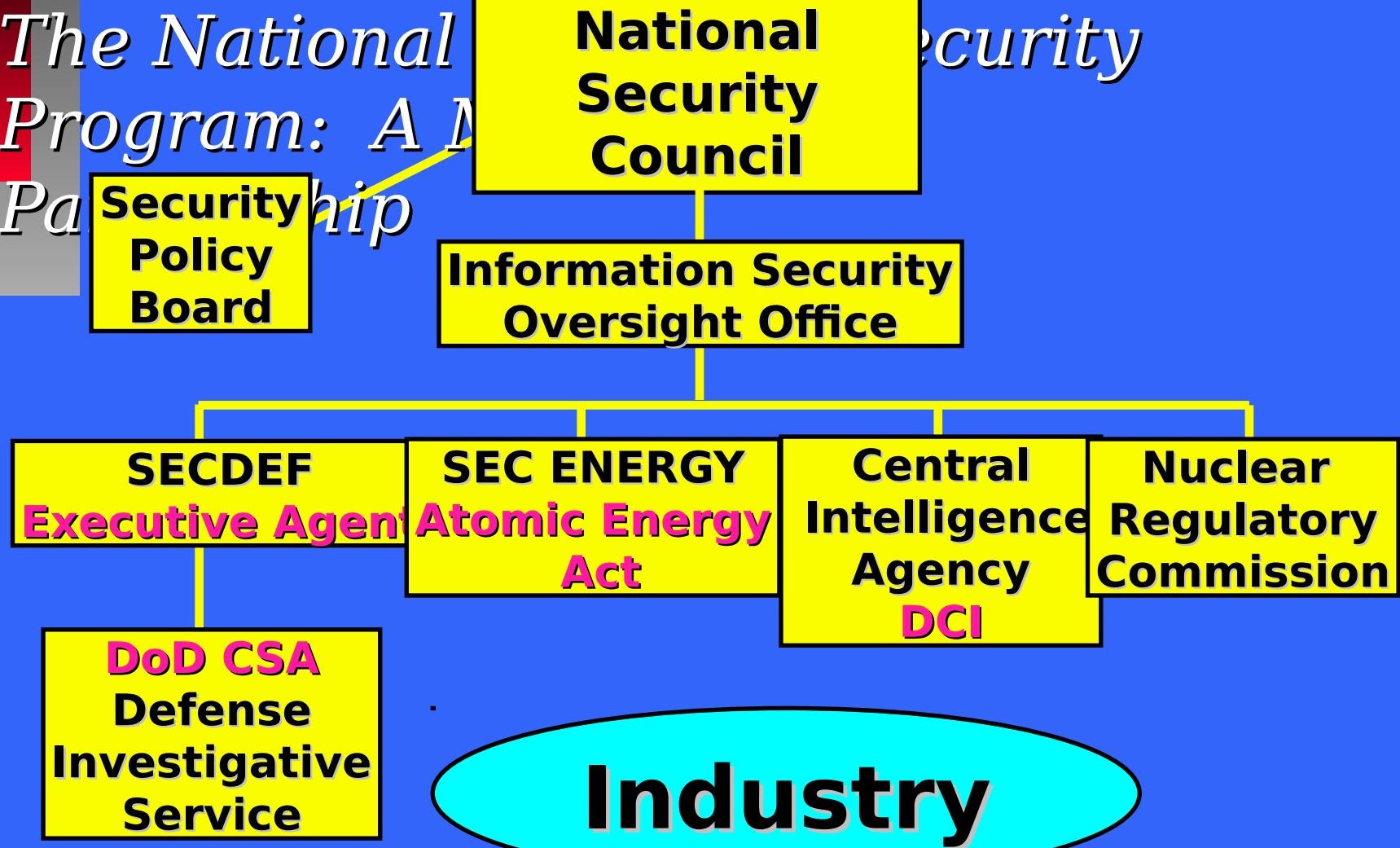
The Industrial Security Program:

- **Event-driven security reviews, COMSEC Account reviews and advice and assistance to industry**
- **CI threat information and security education to industry**
- **Assistance to UAs on industrial security matters, including security assessments for contractors located on government sites**
- **Review and adjudication of FOCI cases for cleared facilities**
- **Inquiries into security violations resulting in the loss or compromise of classified information**

DIS' Government Customers



The National Security Program: A Partnership



The “NISPOM”

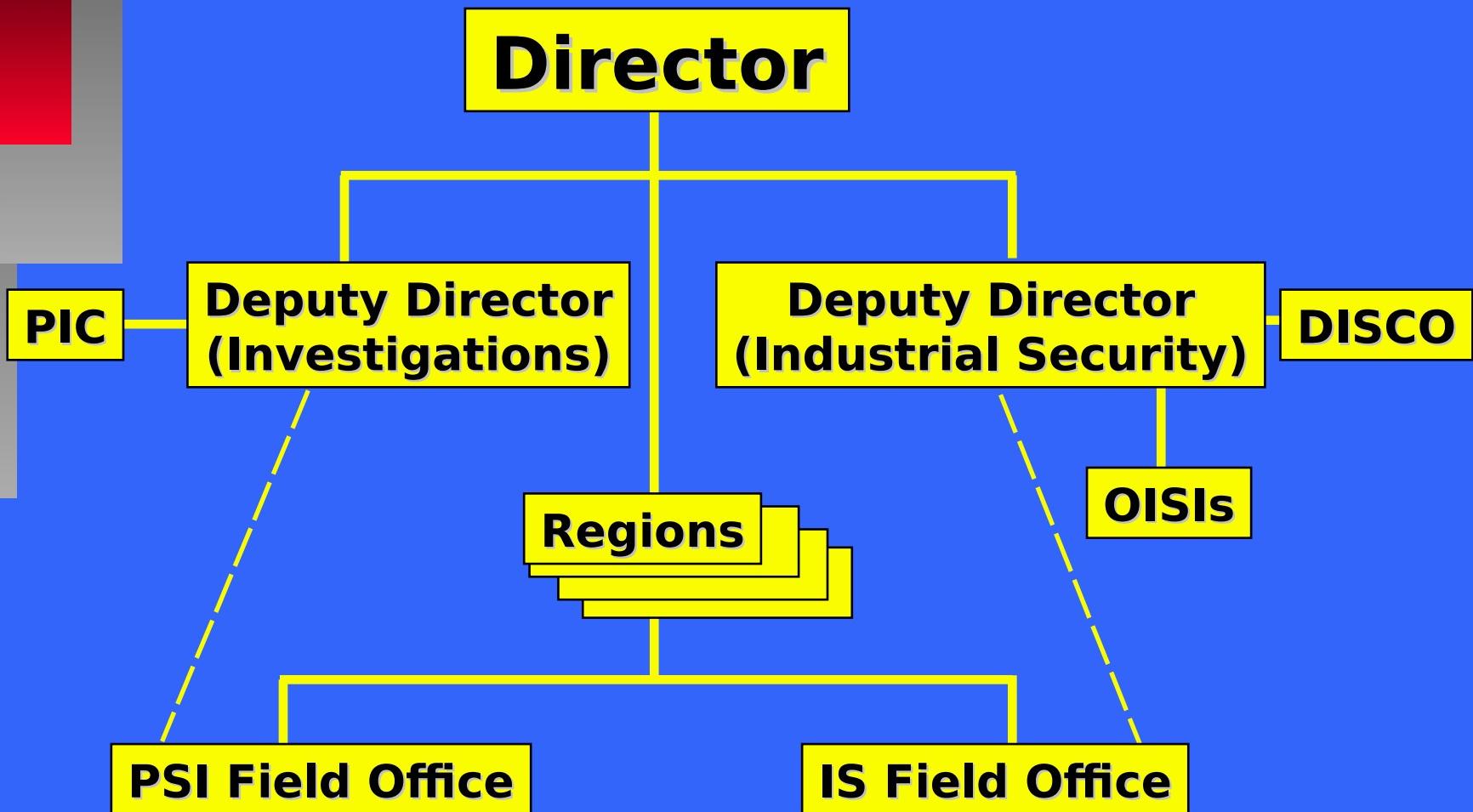
- ***NISP Operating Manual***
- ***Published by SECDEF as Executive Agent for the NISP***
- ***Four Signatories: DoD, DoE, CIA, NRC***
- ***Describes Industry's responsibilities for protecting classified information***

The DIS Team: A Government/Industry Partnership

***Support for the NISP
comes from three
sources:***

- ***DISCO***
- ***DIS Field Elements***
- ***DoDSI***

Organization of the Defense Investigative Service



What is Industrial Security?

- ***Element of information security program***
- ***Protection of Government classified information in the custody of Industry***
- ***Often an essential component of the Acquisition Systems Protection Program (ASPP)***

Acquisition Systems Protection Defined:

- *Tailored application of countermeasures to specific threats and vulnerabilities of an acquisition program*
- *Produces a cost-effective, secure environment for DoD critical technology throughout the procurement process*

Background: The Acquisition Systems Protection Program (ASPP)

(1991) DoD Directive 5000.1, “Defense Acquisition,” and DoD Instruction 5000.2, “Defense Acquisition Policies and Procedures,” established the ASPP within the DoD

ASPP *cont.*

- **(1994) DoD Manual 5200.1-M: Applied risk management theory to ASPP**
- **(1994) Joint Security Commission Report: Set future direction of national security efforts**

Core of the ASPP Concept: “EPITS”

***Identification of
Essential Program
Information, Technology,
or Systems (EPITS) for
each acquisition
program***

Assessing the Risk: The “PPP”

Once EPITS are identified:

- Intel Community IDs countries which have an interest and capability to collect information***
- ***Security Specialists identify program's vulnerabilities***
- ***Program Protection Plan (PPP) formulated: Outlines plan for security of the system throughout its life cycle***

The PPP: A Single Source Plan for Security of the System Throughout its Life Cycle

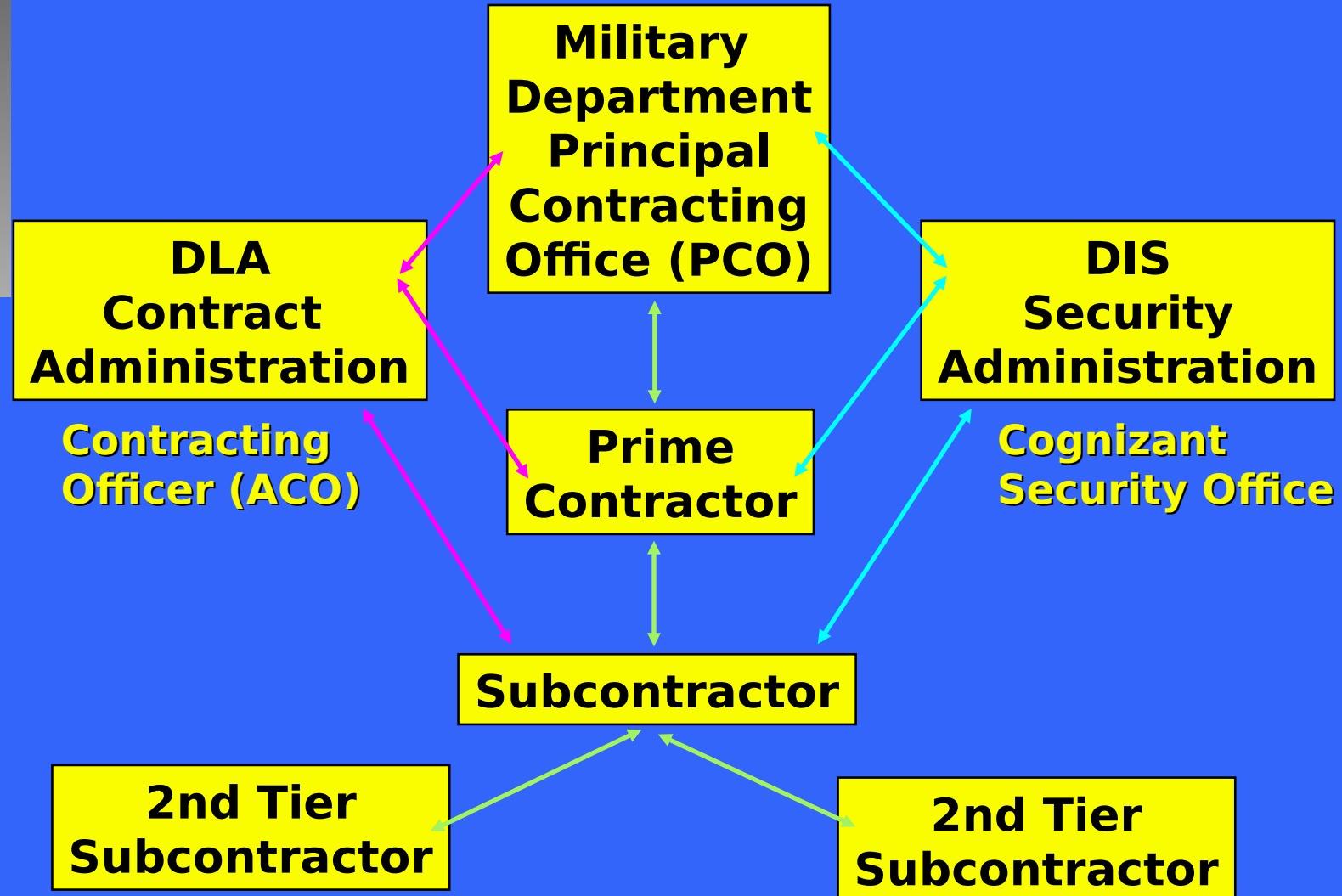
- ***Consists of a Technology Assessment/Control Plan***
- ***Time-or event-phased Security Classification Guide***
- ***System Security Engineering Management Plan***

The Role of DIS and the UA in the Acquisition Process

Relationship begins when a determination is made that industry will require access to classified information at one or more stages in the acquisition process, i.e., solicitation, bid/proposal, evaluation, award or delivery

Contract Relationships

Classified Contract



Security and the Acquisition Process

- ***Security must be considered at the outset***
- ***Failure to address security concerns impacts upon cost and performance***
- ***Good communication between contracting, security personnel and program managers is essential***
- ***Security classification guidance is responsibility of the Program Manager***

Security and the Acquisition Process

- **Allow adequate time to clear uncleared firms or upgrade existing facility clearances**
- **DIS IS Reps conduct facility clearance surveys to determine firm's eligibility for a facility clearance**
- **FCLs can take anywhere from 3-6 months or longer**

Key FCL Criteria

- ***Key Management Personnel (e.g., President, Chairman of the Board, Facility Security Officer) must be cleared***
- ***Any Foreign Ownership, Control or Influence (FOCI) must be adjudicated and mitigated***

Facility Clearance (FCL) Concept

- ***In order for employees of a business entity (e.g., corporation) to have access to classified, entity must have FCL***
- ***In order for operating location of entity (e.g., division) to have possession of classified, FCL and safeguarding capability required***

Basic Requirements for a Facility Security Clearance

- ***Contractor must require access to classified information***
- ***Contractor must be organized and existing under state law, and must be located in the U.S. or its territorial areas or possessions***
- ***Contractor must have a reputation for integrity and lawful conduct in its business dealings***
- ***The contractor and its key managers must not be barred from participating in Government***

DoD Security

Agreement

Contractor Agrees

- ***Establish an effective industrial security program***

Government Agrees

- ***Classify information***
- ***Grant clearances***
- ***Assist contractor facilities***

Allows termination by either party with 30 days notice

Contracting Officer Responsibilities

- **Determine need for contractor to have access to classified information**
- **Verify clearance status of perspective contractor**
- **If contractor does not have a facility clearance or safeguarding capability, request DIS take clearance action**
- **Unnecessary clearance actions are costly and divert DoD resources**

Contracting Officer Responsibilities

- ***RFQs, RFPs, IFPs and IR&D solicitations must accurately reflect the security requirements both for the procurement process and contract performance***
- ***Include in Statement of Work***
- ***DFAR imposes security requirements on contractors***

Where Are Requests for Facility Security Clearances Submitted?

- **Requests for new FCLs are submitted to the Facility Clearance Branch (S0834) at the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio.**
(614) 692-5255/5256/5257
- **FAX: (614) 692-5260/1110**
- **FCLs Verified by Central Verifications Activity (410) 865-2720/2721**

Contracting Officer Responsibilities cont.

- **Provide contractor security classification guidance - Incorporate in the DD Form 254**
- **PCO or his/her representative signature required**
- **Include original DD Form 254 with every RFQ, RFP, IFP, other solicitation or follow-on contract**
- **Issue final DD Form 254 upon final delivery of goods or services or on termination of contract**

Contracting Officer Responsibilities: The DD Form 254

- ***Identifies security requirements and classification guidance needed to receive, protect and respond to the solicitation request, and/or perform on a classified contract***
- ***Indicates clearance level for overall tasking and safeguarding requirements if any***

The DD Form 254 cont.

- ***Special Access Program (SAP) Information?***
- ***Use of ADP equipment to process classified?***
- ***Sensitive Compartmented Information (SCI)?***
- ***Communications Security (COMSEC)?***
- ***Access to classified overseas?***
- ***Other requirements unique to the program or procurement?***
- ***Identify cognizant DIS industrial security field office***

Contracting Officer Responsibilities *cont.*

- ***Periodically review security requirements with program office. Issue revised DD Form 254 if significant changes occur***
- ***Review/respond to contractor requests for public release***
- ***Tailor DD Form 254 to contract performance***
- ***If “follow-on” contract, reference classification guidance for preceding contract in the DD Form 254***

Contracting Officer Responsibilities: Special Situations

- **Basic Ordering Agreements** - A single DD Form 254 may be issued unless product/services require specifications different from that provided for overall contract
- **Contracts Requiring Limited Classification Guidance** - Contracts which involve no actual knowledge/generation of classified but individuals need to be present in areas accessible to classified - ACO/PCO signature is not required when issued by Prime to Sub

Contracting Officer Responsibilities: Subcontracting

- **If Prime employs a Sub, they issue a DD Form 254 to Sub**
- **“254” must address all critical issues**
- **Questions of adequacy must be resolved between Prime, Sub, Contracting and/or UA Program Office**

Contracting Officer Responsibilities: Regrading & Declassification

- ***Timely notification to contractor of regrading or declassification actions.
May require reissuance of DD Form 254***
- ***If unclassified material (previously released to contractor) is upgraded to classified, advise via U.S. Certified Mail or secure communications***
- ***Resolve classification guidance problems.
Often requires assistance/intervention of UA program office***

The DD Form 254 *cont.*

Minimum Distribution:

- ***ACO***
- ***Prime Contractor***
- ***Subcontractor (if applicable)***
- ***Local DIS IS Office of the Prime and Subcontractor***

The Goal: Security that is Threat-Appropriate, Rational & Cost-Effective

- **Threat-Appropriate:** *Countermeasures appropriate to known or suspected threats*
- **Rational:** *A “common sense” approach to problem solving*
- **Cost-Effective:** *Balance between effective security countermeasures and relative costs*

DIS Counterintelligence Initiative

***“A critical element
necessary to make smart
security decisions is
reliable, usable,
intelligence data
defining the threat”***

Redefining Security
***a report by the Joint Security
Commission***

DIS CI Integration Initiative cont.

Authorized in 1994 by ASD (C3I)

Objectives:

- **Integrate CI with DIS' SCM mission**
- **Infuse CI experience & knowledge**
- **Support Industry's involvement in the international market while increasing awareness**
- **Assist industry in recognizing and reporting instances of suspected foreign intelligence collection activities**

DIS CI Integration Initiative cont.

- **Personnel Security Investigations:** Early identification and referral of cases involving possible espionage
- **Industrial Security:** Provide industry with answers to:
 - Who is targeting us?
 - What are they targeting?
 - What are the MO's being used?

Industry Plays an Important Role:

- ***Contractors are required to report efforts to obtain illegal or unauthorized access to classified information or to compromise a cleared employee***
- ***Enables the development of “threat profiles” for individual facilities***
- ***Assists the Intel Community in determining what the***

CI Ongoing & Future Initiatives

- ***Focus on contractor facilities/employees with frequent contacts with foreign interests***
- ***Assist in the provision of appropriate threat information for individual contractor facilities***
- ***Facilitate coordination with local CI community***

Other Supported Programs

- ***Key Asset Protection Program (KAPP) - DIS assists FORSCOM by conducting surveys and site visits of DoD assets critical to production and mobilization, deployment and military operations***
- ***IS Reps assess each site's vulnerability to sabotage and other hostile or destructive acts***

Other Supported Programs

- **Arms, Ammunition & Explosives (AA&E) Program**
 - *DIS supports the DoD AA&E Program by assessing contractor compliance with the physical security provisions contained in contracts involving sensitive conventional AA&E*
- *IS Reps conduct on-site inspections of contractors identified by the Military Departments to assess their ability to protect sensitive AA&E*

DIS Oversight of Special Access Programs

- *DIS' involvement in SAP oversight continues to expand*
- *Largest customer is the U.S. Army, which has turned over all its procurement SAPs to DIS*
- *DIS IS Reps oversee protection of critically sensitive program information, assess physical safeguards, provide security education, and collaborate with SAP SPO/PMO to ensure effective and cost effective SAP security*

Industrial Security International Mission

- ***Delegated DoD responsibility regarding industrial security issues resulting from bilateral security agreements***
 - *Implementation of security requirements for foreign government classified contracts*
 - *Serve as government representative in import/export.*
 - *Primary focal point for foreign governments on industrial security issues*
- ***Specific role identified in ITAR relative to transfer of classified information***
 - *Ensure what is being transferred is consistent with export approvals*
 - *Ensure appropriate supporting security measures are in place*
 - *Facilitate the exchange*

The Offices of Industrial Security International (OISI)

- ***Assist U.S. industry overseas through offices in Belgium, Germany, Melbourne FL, and San Diego CA. Primary source for security training in high threat locations***
- ***Offices of record for personnel security clearance and security assurance data on U.S. contractors assigned in their regions***
- ***Provide liaison to U.S. Military and civilian agencies***
- ***Conduct security briefings and provide CI threat data***

DIS Provides A Unique Government Service . . .

***By lending our industrial security,
personnel security and AIS
security expertise to assist in the
protection of classified
information critical to the
preservation of our nation and its
economic future.***

***For nearly 25 years DIS has
provided a full range of security
countermeasures assurances to
government and industry. We
look forward to providing our
expert assistance to you.***